BEST AVAILABLE COPY

REMARKS

In the Office Action, the Examiner rejected Claims 1-21, which are all of the pending claims, under 35 U.S.C. 103 as being unpatentable over the prior art. Specifically, Claims 1-16, 18 and 20 were rejected as being unpatentable over U.S. Patent 6,519,700 (Ram) in view of U.S. Patent 6,247,127 (Vandergeest); and Claims 17, 19 and 21 were rejected as being unpatentable over Ram in view of Vandergeest and further in view of U.S. Patent 6,775,655 (Peinado).

Applicants herein ask that independent Claims 1, 6, 10, 14, 18 and 20 be amended to better describe the subject matters of these claims.

For the reasons discussed below, the Examiner is asked to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-21 under 35 U.S.C. 103, and to allow these claims.

The instant invention relates to digital rights management (DRM) systems, and more specifically, relates to a DRM that is basically transparent to the application with which the system is used – that is, the DRM does not interfere with the application development.

The present invention includes three major components: a verification system, a trusted content handler, and a user control interface. The verification system verifies certain properties of programs that are executing or that are about to be executed. The trusted content handler performs the main tasks of content decryption and feed, and the user control interface ensures that user interactions with the player interactions do not violate usage rights.

11

An important aspect of the invention is that the certificate generator generates a certificate after inspecting the application code and determining that certain required properties have been met by that application code. Moreover, components of the verification system, the trusted content handler, and the user interface control operate independently from the player application, reside locally in an end-user device having said player application, and are dynamically linked to that application at runtime.

In this way, the invention provides a digital rights management system that is completely transparent to the player/viewer application running on the client host system. The invention controls access to the content and constrains it according to the rights and privileges granted to the user during the content acquisition phase, without interfering with the design or development of the application.

The references cited by the Examiner relate to document or Internet security, but they do not disclose or suggest the DRM system of the present invention.

For instance, Ram, et al. describes a procedure for distributing electronic documents. With this procedure, a self-protecting document is used that contains an encrypted document, a secure set of permissions, and the software needed to process the document. As disclosed in Ram, et al, by combining an encrypted document with a set of permissions and an executable code segment that includes most of the software necessary to extract and use the encrypted document, the self-protecting document accomplishes protection of document contents without the need for additional hardware and software.

Vandergeest describes a procedure for secure off-line communications. Generally, in this procedure, information is exchanged between two end-users to enable them to go off lien and participate in secure communications.

12   G:\IBM\105\13873\AMEND\13873.am3.doc

The Examiner particularly relied on Vandergeest for its disclosure of an off-line verifier to verify that player applications have certain properties. As explained from column 3, line 66 to column 4, line 7 of Vandergeest, this verification is made by checking a directory to obtain a certificate. Thus, with the procedure disclosed in Vandergeest, this certificate is obtained, but not generated.

Independent Claims 1, 6, 10, 14, 18 and 20, as presented herewith describe important feature of the invention not shown in or suggested by the prior art. In particular, Claims 1, 6 and 10 describe the feature that the user interface ensures that the user interaction with the player applications does not violate usage rights by intercepting and filtering messages sent from the user to the player applications in accordance with a user rights set obtained by the user.

Claims 14, 18 and 20 are directed, respectively, to a code identity and integrity verification system, to a method for verifying the identity and integrity of code, and to a program storage device for verifying code identity. These claims describe the feature that an authenticator, which is used to verify that requests from player applications have been authorized, operates independently from the applications, resides locally in an end-user device having the applications, and is dynamically linked to the applications at run-time.

The above-discussed features of the invention are of utility because they enable a digital rights management system that effectively manages digital rights, and at the same time is very flexible and minimally intrusive, and does not put any conditions on the type of the contents that need to be delivered, or on the applications used to access those contents.

13

The other references of record have been reviewed, and these other references, whether considered individually or in combination, also fail to disclose this use of the certificate generator.

Because of the above-discussed differences between Claims 1, 6, 10, 14, 18 and 20 and the prior art, and because of the advantages associated with those differences, Claims 1, 6, 10, 14 and 18 patentably distinguish over the prior art and are allowable. Claims 2-5 are dependent from Claim 1 and are allowable therewith; and Claims 7-10 are dependent from, and are allowable with, Claim 6. Also, Claims 11-13 are dependent from Claim 10 and are allowable therewith; and Claims 15-17 are dependent from Claim 14 and are allowable therewith. Claims 19 and 21 are dependent from, and are allowable with, Claims 18 and 20, respectively.

The changes to the claims that are requested herein only emphasize features already set forth in those claims. For instance, Claim 1 presently includes a verification system, a content handler, and a user interface; and the amendments requested herein describe in more detail how the user interface operates, and how the verification system, the content handler and the user interface are able to achieve the above-discussed transparency. It is thus believed that entry of this Amendment is appropriate, and such entry is respectfully requested.

14   G:\IBM\105\13873\AMEND\13873.am3.doc

In light of the above-discussion, the Examiner is respectfully requested to enter this Amendment, to reconsider and to withdraw the rejection of Claims 1-21 under 35 U.S.C. 103, and to allow these Claims. If the Examiner believes that a telephone conference with Applicants' Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,

John S. Sensny
Registration No. 28,757
Attorney for Applicants

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343
Customer No. 23389

JSS:jy

15   G:\IBM\105\13873\AMEND\13873.am3.doc